UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/075,471 | 02/13/2002 | Jeffrey M. Ayars | REAL-2006051 (RN65) | 7533 |

61857 7590 03/24/2009
AXIOS LAW GROUP, PLLC / REALNETWORKS, INC
1525 4TH AVE, STE 800
SEATTLE, WA 98101-1648

| EXAMINER | |
|---|---|
| PALIWAL, YOGESH | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2435 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 03/24/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Continuation of 11: The request for reconsideration has been considered but does NOT place the application in condition for allowance because Applicant's arguments filed 03/06/2009 have been fully considered but they are not persuasive for the following reasons:

Regarding Independent claim 25, applicant argues that, “Applicants respectfully submit that England does not disclose at least the following elements of Claim 25: "rendering in part.., said first digital content; re-verifying.., that one of the [immediate downstream modules] is uncompromised; and transferring.., the first digital content to the re-verified immediate downstream module to further the rendering of the first digital content." Indeed, as set out in the passage from col. 14, above, England at best discloses merely a single verification step, "block 544 [verifies] that its signature is correct .... "England never discloses that a root digital content rendering module verifies downstream modules, re-verifies a downstream module, and transfers the partly rendered digital content to the re-verified downstream module for further rendering, as claimed in Claim 25.”

In reply, examiner would like to point out that England clearly discloses a root digital content rendering module verifies downstream modules at least at (see Fig. 4, and also Column 11, lines 9-14, “As a practical matter, this can be accomplished by placing binary resources in a CP secure DLL such as 441 that name the digest or public key of other trusted modules. Upon initial load--or later--the SM identifies the trusted modules, so that a call to them maps their pages.”) and re-verifying a downstream module, and transfers the partly rendered digital content to the re-verified downstream module for further rendering (see, Column 8, lines 25-35, “The secure content-provider module 441, receiving trust from security manager 420, in turn entrusts a further, lower level of trust in other modules. In this case, the audio application confers trust upon a named audio-card driver module 450, which in turn names a secure portion 461 of the computer's audio processing stack 460 as worthy of trust for processing the premium audio content".) As disclosed by Column 11, lines 9-14, SM identifies the trusted modules during an initial load, this is what examiner is interpreting as verification step and once the audio content is downloaded SM once again verify a downstream modules (such as secure content-provider module, audio-card driver module, and so on). Claim only calls for "rendering in part with said root one of said modules said first digital content" and England at Columns 11, lines 6-31 and also Column 9, lines 7-13, clearly discloses this feature ("A convenient way is to allow the content distributor to encrypt a data block that contains its keys or other secret data, and that names the digest or signer of the target secure content-provider module. The CP alone is able to decrypt the secrets, and only gives the secrets to the named CP or to a CP that meets the requirements of trust." "However, current application and OS architectures require multiple modules to work cooperatively in processing and rendering content. For example, an application program might decrypt audio, hand it to an OS component to be decompressed, which then hands the decompressed audio to a further component to send the audio data to the output device.")

Applicant further argues that, "Col. 8 lines 25- 35 are directed towards merely identifying trustworthy modules, not verifying and also re- verifying modules, as claimed in Claim 25. Col. 11 lines 6-31 are directed towards merely providing cryptographic services by a security manager, not a digital content rendering module, for identifying, not verifying, a trusted module, not a digital content rendering module."

Applicant's argument that England only identify and does not verify or re-verify modules is not found persuasive because England clearly discloses "For example, a first module trusted by a content distributor for handling the digital content may designate another module specified by the first module as trusted for handling the digital content, where the other module is a hardware device, the first module verifies the identity of the hardware device and the first module grants access to a designated memory area to the hardware device. Trust can be established declaratively or programmatically, by naming the public key, digest, or other signature of other applications or modules that have access to some or all of their code or data in the secure storage." This part clearly discloses that upper modules simply does not identify the lower module but utilizes public key, digest or other signatures of the modules to perform both the identification and verification.

For at least the above reasons, it is believed that the rejection is maintained.

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435